

## **U.S. Privacy Laws**

### **Privacy Act of 1974**

Places limitations on the disclosure of information in a system of records maintained by a federal agency (or its contractors) without the written request or consent of the individual to whom the record pertains. Agencies are permitted to disclose information for purposes discussed during the original collection by identifying it as a “routine use” and publishing notice of it in the Federal Register.

### **E-Government Act of 2002, Title II and III**

Requires agencies assess the impact on privacy for systems that collect personally identifiable information (PII), known as a privacy impact assessment (PIA).

### **Graham-Leach Bliley Act (GLBA)**

Requires U.S. “financial institutions” to establish administrative, technical, and physical information safeguards to ensure the confidentiality and integrity of customer records and information.

### **Health Insurance Portability & Accountability Act (HIPAA)**

Requires “covered entities” to implement privacy and security standards for health information at every level of the healthcare system.

### **Children's Online Privacy Protection Act (COPPA)**

Requires parental consent for certain websites who knowingly collect PII on children under the age of 13.

### **Fair Credit Reporting Act**

Helps ensure that consumer reporting agencies act fairly, impartially, and with respect for the consumer's right to privacy when preparing consumer reports on individuals.



## **For More Information**



Below is a sampling of websites regarding your online privacy at home and at work.

#### **General Information:**

<http://www.ftc.gov/privacy/index.html>  
<http://www.i-safe.org/>  
<http://www.getnetwise.org/>  
<http://www.staysafeonline.org/>

#### **ID Theft/Fraud :**

<http://www.consumer.gov/idtheft/>  
<http://www.lookstoogoodtobetrue.com/>  
<http://www.onguardonline.gov/>

#### **Credit Reports :**

<http://www.annualcreditreport.com>  
<http://www.equifax.com/>  
<http://www.transunion.com/>  
<http://www.experian.com/>

#### **Combating Spam/Telemarketing:**

<http://www.ftc.gov/spam/>  
<https://www.donotcall.gov/>

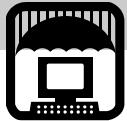
#### **Kid's Privacy:**

<http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/>  
<http://www.netsmartzkids.org/>  
<http://www.ikeepsafe.org/>  
<http://www.mcgruff.org/>



 Please contact to the ITSC Help Desk at (866) 699-4872, for more information on how to protect your privacy at work.

## **Protecting Yourself Online Memorandum**



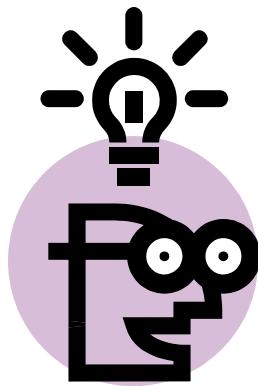
The recent theft of \$35,000 from the Federal Thrift Savings Plan (TSP) accounts of 25 individuals, including Department of Health and Human Services (HHS) personnel, highlights the ongoing need for personal vigilance when using HHS computer resources, as well as ensuring that your home computer systems are protected. Recent attacks on the TSP website highlight the growing sophistication and organization of internet crime. Criminal computer activity is no longer restricted to the disgruntled hacker, but is increasingly an organized and for-profit enterprise aimed at gaining access to online financial accounts of all types. Through network and computer-based solutions, HHS provides a high level of security while working in the office. While working from home provides flexibility in completing work related activities, there is an inherent loss of protection when working from outside of HHS's network.

To a large degree, your computing practices and browsing behavior determine how vulnerable your personal information is to criminal activity. Online criminals work to exploit the latest holes in common internet software before users can patch them or even before the manufacturer has released repairs. For this reason it is important that you implement a variety of personal security solutions to stop intruders and unwanted activity. Even with the best technology in place, criminals can still possibly get your personal information. Deception is one of the primary means of exploiting even the most informed user. Whether being asked to inadvertently install software that will capture passwords you type into your computer, or to fill in an account number on a website, the ultimate defense is you. It is best to maintain a wary attitude of any unsolicited email or pop-up advertisements.



## Privacy Fun Facts

- The U.S. Constitution does not explicitly guarantee privacy. The right to privacy has been established through various Supreme Court decisions.
- The predecessor to HHS (Department of Health, Education, and Welfare) commissioned a report in 1973 that had a significant influence on creating the Privacy Act of 1974.
- It is safer to transmit information online from a website using https:// rather than http://.
- When a breach occurs and personal information has been compromised, only certain states, such as California, require businesses to inform consumers. There is no federal law requiring disclosure of the breach.
- Just because you delete your website history, does not mean other people can't see the websites you've visited. Most of what your computer tracks is not visible and cannot be deleted manually.
- When using an internet browser, you have the option of determining your privacy settings. For most internet browsers, you can find your privacy choices under "Options".



To stay current about privacy or to learn more, visit the HHS Privacy Intranet page at:  
<http://intranet.hhs.gov/infosec/privacy.html>



# Protecting You and Your Family Online



For more information, visit the Secure One HHS intranet site at:  
<http://intranet.hhs.gov/infosec/>

